

process becomes a matter of public record.

(b) Before disseminating any record about any individual to any person other than an Endowment employee, the Endowment shall make reasonable efforts to ensure that such records are, or at the time they were collected were, accurate, complete, timely, and relevant for Endowment purposes. This paragraph (b) does not apply to disseminations made pursuant to the provisions of the Freedom of Information Act (5 U.S.C. 552) and paragraph (a)(2) of this section.

§ 1159.14 Will the Endowment maintain a written account of disclosures made from its systems of records?

(a) The Office of the General Counsel shall maintain a written log containing the date, nature, and purpose of each disclosure of a record to any person or to another agency. Such accounting shall also contain the name and address of the person or agency to whom each disclosure was made. This log need not include disclosures made to Endowment employees in the course of their official duties, or pursuant to the provisions of the Freedom of Information Act (5 U.S.C. 552).

(b) The Endowment shall retain the accounting of each disclosure for at least five years after the accounting is made or for the life of the record that was disclosed, whichever is longer.

(c) The Endowment shall make the accounting of disclosures of a record pertaining to you available to you at your request. Such a request should be made in accordance with the procedures set forth in § 1159.8 of this part. This paragraph (c) does not apply to disclosures made for law enforcement purposes under 5 U.S.C. 552a(b)(7) and § 1159.13(a)(7) of this part.

§ 1159.15 Who has the responsibility for maintaining adequate technical, physical, and security safeguards to prevent unauthorized disclosure or destruction of manual and automatic record systems?

The Deputy Chairman for Management and Budget has the responsibility of maintaining adequate technical, physical, and security safeguards to prevent unauthorized disclosure or de-

struction of manual and automatic record systems. These security safeguards shall apply to all systems in which identifiable personal data are processed or maintained, including all reports and outputs from such systems that contain identifiable personal information. Such safeguards must be sufficient to prevent negligent, accidental, or unintentional disclosure, modification or destruction of any personal records or data, and must furthermore minimize, to the extent practicable, the risk that skilled technicians or knowledgeable persons could improperly obtain access to modify or destroy such records or data and shall further insure against such casual entry by unskilled persons without official reasons for access to such records or data.

(a) *Manual systems.* (1) Records contained in a system of records as defined herein may be used, held or stored only where facilities are adequate to prevent unauthorized access by persons within or outside the Endowment.

(2) All records, when not under the personal control of the employees authorized to use the records, must be stored in a locked metal filing cabinet. Some systems of records are not of such confidential nature that their disclosure would constitute a harm to an individual who is the subject of such record. However, records in this category shall also be maintained in locked metal filing cabinets or maintained in a secured room with a locking door.

(3) Access to and use of a system of records shall be permitted only to persons whose duties require such access within the Endowment, for routine uses as defined in § 1159.1 as to any given system, or for such other uses as may be provided herein.

(4) Other than for access within the Endowment to persons needing such records in the performance of their official duties or routine uses as defined in § 1159.1, or such other uses as provided herein, access to records within a system of records shall be permitted only to the individual to whom the record pertains or upon his or her written request to the General Counsel.

(5) Access to areas where a system of records is stored will be limited to

§ 1159.16

45 CFR Ch. XI (10–1–03 Edition)

those persons whose duties require work in such areas. There shall be an accounting of the removal of any records from such storage areas utilizing a written log, as directed by the Deputy Chairman for Management and Budget. The written log shall be maintained at all times.

(6) The Endowment shall ensure that all persons whose duties require access to and use of records contained in a system of records are adequately trained to protect the security and privacy of such records.

(7) The disposal and destruction of records within a system of records shall be in accordance with rules promulgated by the General Services Administration.

(b) *Automated systems.* (1) Identifiable personal information may be processed, stored or maintained by automated data systems only where facilities or conditions are adequate to prevent unauthorized access to such systems in any form. Whenever such data, whether contained in punch cards, magnetic tapes or discs, are not under the personal control of an authorized person, such information must be stored in a locked or secured room, or in such other facility having greater safeguards than those provided for herein.

(2) Access to and use of identifiable personal data associated with automated data systems shall be limited to those persons whose duties require such access. Proper control of personal data in any form associated with automated data systems shall be maintained at all times, including maintenance of accountability records showing disposition of input and output documents.

(3) All persons whose duties require access to processing and maintenance of identifiable personal data and automated systems shall be adequately trained in the security and privacy of personal data.

(4) The disposal and disposition of identifiable personal data and automated systems shall be done by shredding, burning or in the case of tapes or discs, degaussing, in accordance with any regulations now or hereafter proposed by the General Services Administration or other appropriate authority.

§ 1159.16 Will the Endowment take steps to ensure that its employees involved with its systems of records are familiar with the requirements and implications of the Privacy Act?

(a) The Chairperson shall ensure that all persons involved in the design, development, operation or maintenance of any Endowment system are informed of all requirements necessary to protect the privacy of subject individuals. The Chairperson shall also ensure that all Endowment employees having access to records receive adequate training in their protection, and that records have adequate and proper storage with sufficient security to assure the privacy of such records.

(b) All employees shall be informed of the civil remedies provided under 5 U.S.C. 552a(g)(1) and other implications of the Privacy Act, and the fact that the Endowment may be subject to civil remedies for failure to comply with the provisions of the Privacy Act and these regulations.

§ 1159.17 Which of the Endowment's systems of records are covered by exemptions in the Privacy Act?

(a) Pursuant to and limited by 5 U.S.C. 552a(j)(2), the Endowment system entitled "Office of the Inspector General Investigative Files" shall be exempted from the provisions of 5 U.S.C. 552a, except for subsections (b); (c)(1) and (2); (e)(4)(A) through (F); (e)(6), (7), (9), (10), and (11); and (i), insofar as that Endowment system contains information pertaining to criminal law enforcement investigations.

(b) Pursuant to and limited by 5 U.S.C. 552a(k)(2), the Endowment system entitled "Office of the Inspector General Investigative Files" shall be exempted from 5 U.S.C. 552a(c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f), insofar as that Endowment system consists of investigatory material compiled for law enforcement purposes, other than material within the scope of the exemption at 5 U.S.C. 552a(j)(2).

(c) The Endowment system entitled "Office of the Inspector General Investigative Files" is exempt from the above-noted provisions of the Privacy Act because their application might